

OpenAM 10.20 Snapshot版

新機能紹介



OSSTech

2013年4月12日

オープンソース・ソリューション・テクノロジー株式会社

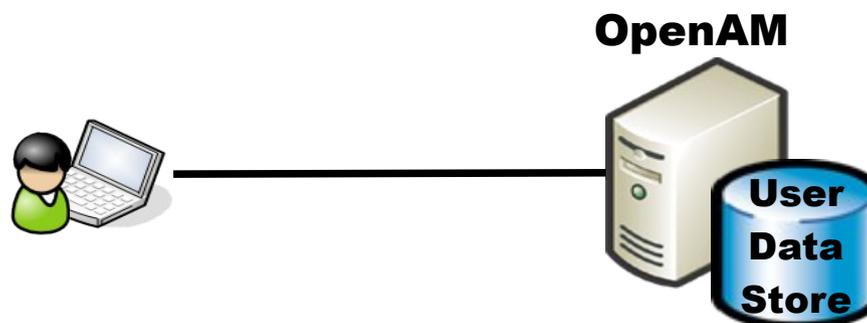
<http://www.osstech.co.jp/>

お問い合わせ info@osstech.co.jp

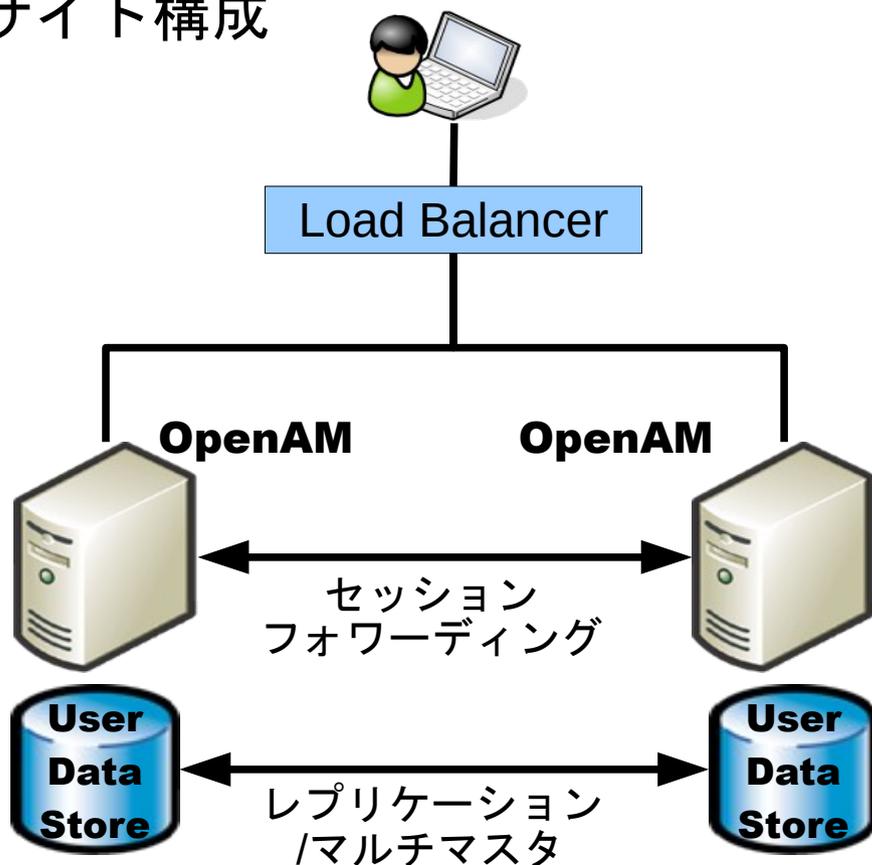
- セッション・フェイルオーバーの改良
 - 設定が飛躍的に容易になった
 - OpenDJのレプリケーション機能を使用
- OATH準拠した認証方式の追加
 - Googleの2段階認証と同じ仕組み
 - 強固な認証を安価に実現可能
- OAuthプロバイダのサポート
 - OpenID Connectに向けた基盤の準備

セッション・フェイル・オーバー (SFO)の改良

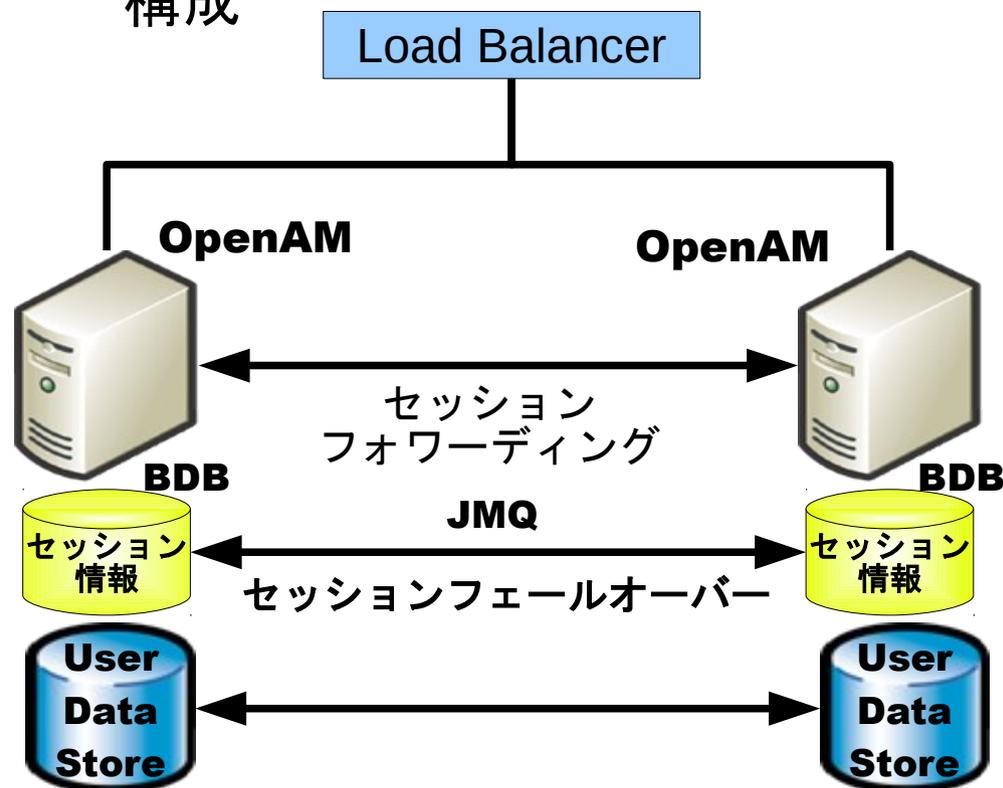
シングルサーバ構成

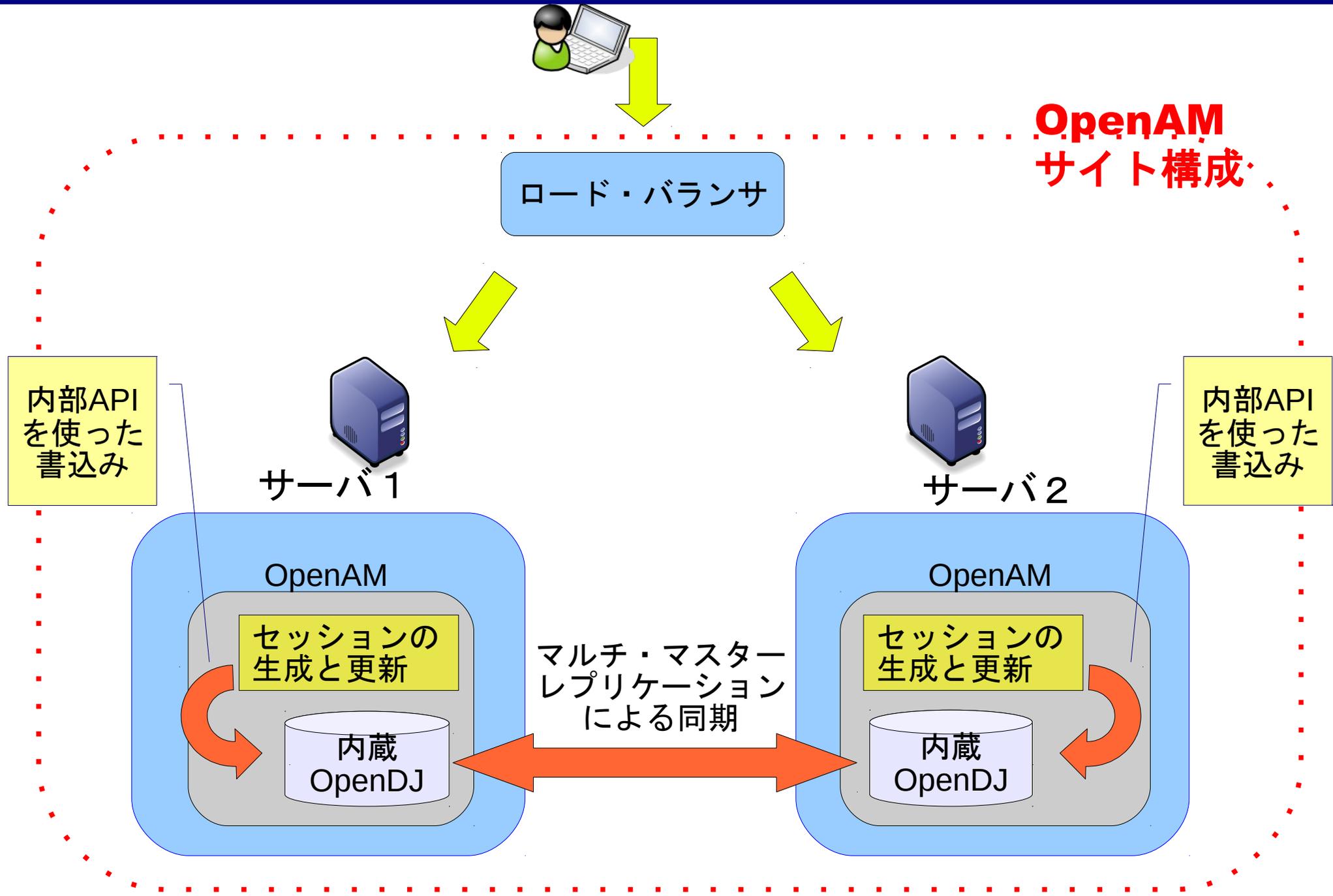


サイト構成



セッションフェールオーバー構成





- 内蔵OpenDJへのセッション情報の書込み
 - サイト構成の場合に設定オプションとして利用可能
 - メモリ上のセッションテーブルも引き続き利用（自分で発行したもののみ）
 - 再起動した場合には、OpenDJからセッション情報を読み込み再構成する
- マルチ・マスタ・レプリケーションによるセッションの冗長化
 - 他のサーバが停止した場合は、そのサーバのセッション情報をOpenDJからメモリ上に再構成しサービスを引き継ぐ

- 難しいことはOpenDJに任せよう！
 - 複数台のサーバにわたるセッションの同期はDirectoryサーバのマルチマスタ・レプリケーション機能で解決
 - メッセージキュー、Berkeley DBは必要無し！
 - OpenAMは必要なセッション情報は全てローカルにあるものとして動作
(個人毎のセッション数の上限値など未実装もあり)
- OpenDJの高い更新性能を利用
 - 内蔵OpenDJ (同じJVM上で動作) へは内部APIを使ってアクセス (デフォルト設定ではログに出ないので注意！)
 - マルチマスタ・レプリケーション処理の効率化

- インストール時に指定

サイト設定の詳細

これは OpenAM の最初のインスタンスで、現在、サイト設定は存在しません。新しいサイト設定を作成するには、次の情報を入力します

* サイト名	<input type="text" value="site01"/>	<input checked="" type="checkbox"/>
	了解	
* ロードバランサの URL	<input type="text" value="http://lb.labnet.com:8080/openam"/>	<input checked="" type="checkbox"/>
	了解	
Enable Session HA Persistence and Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 了解

ここにチェック
するだけ

- Benchmark proves OpenDJ fastest directory server !

(Ludoのブログから引用)

- 第三者による評価(M-Vault)

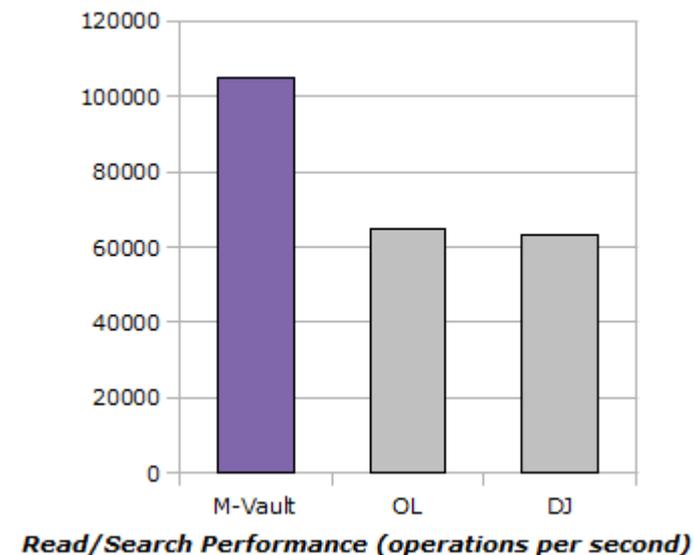
<http://www.isode.com/whitepapers/m-vault-benchmarks.html>

- 内部APIを使った場合はもっと速い (と思われる)

	Modify only (ops/sec)	Search - Modify (ops/sec)	
		Search	Modify
M-Vault	5,000	85,000	3,000
OpenLDAP	7,800	49,000	3,400
OpenDJ	10,000	55,000	4,200

- ところで検索性能は？

- M-Vaultが最速
- 本当に必要かな??



OATHとyubikey への対応

オープンな認証仕様(**O**pen **AuTH**entication)

2種類のワンタイム・パスワード方式

- TOTP — 時刻ベース
 - ✓ 一定間隔 (default: 30 sec) で新しいパスワードを生成
 - ✓ カウンタ : 時刻
- HOTP — イベント (カウンタ) ・ベース
 - ✓ ログインの度に新しいパスワードを生成
 - ✓ カウンタ : 生成回数

様々なサービスが認証強化のために

ワンタイム・パスワードを採用

- Google : 2段階認証
 - メール、アプリ、電話、予備用のパスワード発行
- facebook : ログイン承認
 - メール、アプリ
- Yahoo! Japan : ワンタイム・パスワード
 - メール、アプリ
- Apple : 日本ではこれから導入予定

- 標準化されたトークン・アプリの利用

- スマートフォン上で動作、新たに購入する必要無し
- OATH準拠のものなら何でもOK
 - Google Authenticator (Google認証システム)
 - Android Tokenなど



- 2段階認証を簡単に実現

- 落としても大丈夫
- OpenAMの認証連鎖を使って簡単に構築

- yubikey等のハードウェアトークンもサポート

- 第1段階：ユーザIDとパスワードで認証



OpenAMへのサインイン

OpenAM

ユーザー名:

パスワード:

ログイン

- 第2段階：ワンタイム・パスワードで認証



このサーバーは OATH 認証を使用します

OpenAM

ワンタイムパスワード:

OTP コードを送信

- TOTP, HOTPの両方に対応
 - メールおよびOATH準拠のデバイスをサポート
 - 電話、予備用パスワードの発行は出来ない
- 他の認証方式との組合せが可能
 - アタプティブ・リスク認証との組合せ
 - 認証レベルによるアクセス制御
- 初期データの同期は別途必要
 - 共通シークレットをデバイスとサーバのそれぞれに配布、設定する必要あり
 - QRコードを生成してスキャンさせる方法がお勧め

- OATH認証モジュールの設定
 - 秘密鍵の属性名
 - 使用する OATH アルゴリズム : HOTPまたはTOTPを選択
 - カウンタ属性名 (HOTPのみ)
 - 最終ログイン時刻属性名 (TOTPのみ)
- 認証連鎖の設定
 - 第1段階 : Datastore認証(ユーザID/パスワード)
 - 第2段階 : OATH認証
- メールを使う場合は従来と同様(HOTP認証) を使う
 - メールを使うHOTP認証は別モジュールになっているため注意！

OATH

保存 | リセット | 認証へ戻る

* 必須入力フィールド

レールム属性

* 認証レベル:
i この認証モジュールで認証成功時に設定される認証レベルです。

* ワンタイムパスワードの長さ:
生成する OTP の桁数。6桁以上でなければなりません。

秘密鍵の最小桁数:
秘密鍵として許容される16進数文字の桁数。

* 秘密鍵の属性名: ✖
ユーザーの秘密鍵を格納するユーザープロフィール属性の名前。

* 使用する OATH アルゴリズム: HOTP TOTP
i 使用しているデバイスが OTP を生成するために使用するアルゴリズムを選択します。

HOTP ウィンドウサイズ:
i クライアントと再同期するためのウィンドウサイズ。

カウンタ属性名:
ユーザーのカウンタを格納するユーザープロフィール内の属性の名前。HOTP が OATH アルゴリズムとして選択されている場合、これが必須になります。

チェックサム数字の追加: いいえ はい
i OTP にチェックサム数字を追加します。

トランケーションオフセット:
i OTP の生成にオフセットを追加します。

TOTP タイムステップ期間:
i OTP デバイスが OTP を生成するために使用する秒単位の TOTP タイムステップ。

TOTP タイムステップ数:
i OTP を受け取った前後のチェックのためのタイムステップの数。

最終ログイン時間属性: ✖
i ユーザーの最終ログイン時間を格納する属性。TOTP が OATH アルゴリズムとして選択されている場合、これは必須です。

どちらかのアルゴリズムを選択

HOTPの場合はこちらを設定

TOTPの場合はこちらを設定

✖ デモ用に既存の属性を利用しています。

- 共通シークレットの設定

- ランダムに生成されたバイナリデータ
- 「秘密鍵の属性」に16進数表示で設定
- 長さは20バイト（5の倍数）がお勧め（Googleは10バイト）

- カウンタ/時刻の初期値

- “1”を設定（空だとダメ）

- 共通シークレット

- 20 バイトのバイナリデータ : 16 進数表示
- 例 : 6162636465616263646561626364656162636465

- Base32に変換

例 : MFRGGZDFMFRGGZDFMFRGGZDFMFRGGZDF

- 以下のURI形式にフォーマット

otpauth://totp/<ラベル>?secret=<Base32の値>

例 : otpauth://totp/r1user1?secret=MFRGGZDFMFRGGZDFMFRGGZDFMFRGGZDF

- QRコードに変換

- 認証アプリでスキャン



- Yubicoにより開発
 - 本社：スウェーデン
- USBインターフェイス
 - キーボード・デバイスとして認識される
 - パスワードを手で入力する必要がない
- 時計は内蔵していない
 - 単独でTOTPは不可
 - 安価で長持ち
- 関連モジュールをオープンソースで提供
 - OpenAMとの相性が良い



- OpenAMはユーザのニーズを取り込むことにより着実に進化しています。
- 今回、紹介した機能は、簡単に試してみることが可能です。
- 是非、ダウンロードして使ってみて下さい。



OSSTech

オープンソース・ソリューション・テクノロジー株式会社

<http://www.osstech.co.jp/>

お問い合わせ info@osstech.co.jp